ABSTRACT OF THE DISCLOSURE

Intermediate data a_i, b_i, c_i, and d_i are prepared by an intermediate data preparing equipment 4 from a cryptographic key through a nonlinear type function operation and the like, an extended key preparing equipment 5 selects a $[X_r]$, b $[Y_r]$, c $[Z_r]$, and d $[W_r]$ corresponding to the number of stages r from the intermediate data, and rearranges the data as well as conducts that of bit operation to prepare extended keys, whereby an extended key preparing apparatus by which an extended key required in the case where common key cryptosystem is applied can be safely prepared at a high speed, a process for preparing such an extended key, and a recording medium used therefor are provided.